MQ and the use of data set encryption for IBM z/OS v2.2

Tony Sharkey
Published on 30/08/2017 / *Updated on 27/11/2018*

Extensive use of encryption is one of the most effective ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

Recently IBM announced that data set encryption for z/OS V2.2 has become available for download through the IBM Support web site via APAR OA50569.

z/OS data set encryption (DSE) is delivered through z/OS V2.2 PTFs and, along with required hardware, provides enhanced data protection for z/OS data sets, giving clients the ability to encrypt all of the data associated with entire applications and databases, without the need to make application changes and without impacting SLAs.

Additional design advantages provided by z/OS data set encryption are:

- Uses CPACF acceleration in collaboration with Crypto Express for protected key cryptography, enabling cryptographic operations to be HW accelerated while ensuring that key material is not visible in the clear to the OS, Hypervisor, and Application.
- Encrypt data by policy in a way that is aligned with clients' current access control mechanisms, offering a simplified configuration experience.
- Encrypts at-rest data in bulk, performing efficiently at speed and for low-cost.
- Allows data to remain encrypted with keys managed on IBM Z during replication, backup, and migration.
- Can be configured such that encryption keys are owned and managed by a logical organizational environment, providing cryptographic separation between environments.
- Reduce the risks associated with undiscovered or mis-classified sensitive data.
- Encrypting all of the data associated with an application or database can simplify and reduce the cost of compliance.

How does this affect MQ?

MQ's Advanced Message Security (AMS) offering remains the preferred option for the end-to-end protection of messages, including at rest. It also prevents personnel with a legitimate need to manager the MQ system from inadvertently viewing the contents of sensitive messages. However with the new ability to encrypt z/OS data sets, there is the potential for impact to MQ.

There are a variety of z/OS data sets that MQ uses such as BSDS, page set, logs (both active and archive), shared message data sets, plus sequential files for basic configuration.

The new z/OS data set encryption feature allows AES encryption of data contained in named data sets using ICSF and RACF, so preventing visibility of sensitive data from systems administrators with a legitimate need to manage those data sets.

IBM MQ for z/OS does not support use of DSE with the active logs, page sets and shared message data sets (SMDS) that provide the primary persistence mechanisms for IBM MQ messages. Instead, Advanced Message Security provides an end-to-end encryption solution for IBM MQ messaging, which encompasses the entire MQ network, encryption of data in flight and even inside the runtime IBM MQ processes.

The purpose of this blog is to show the different MQ data sets, whether they support data set encryption, and if not, what errors might be seen.

MQ Data set summary

Dataset	**Support data set encryption**	**Notes**
BSDS	Yes	
Sequential	Yes	**Queue Manager usage:** DD CSQINP1 DD CSQINP2 **AMS M-region usage:** DD AMSVARS Note that data set encryption is not supported for PDS or PDSE.
Pageset 0	No	Abend 5C6-00C91400 on queue manager start.
Pagesets 1-99	No	Queue manager starts successfully. On MQPUT, queue manager logs CSQI04I "… ERROR ACCESSING PAGE SET x" and application is returned MQRC 2193 "Pageset Error".
Active Log	No	Queue manager abend 5C6-00E80084 on queue manager start. Occurs at start-up whether the encrypted log is the first or a subsequent one. The abend code is defined as "A resource manager provided notification of an error during queue manager startup notification processing".

		If a new encrypted log is added to the active log ring, for example using the “DEFINE LOG” command the following messages may be logged: • CSQJ104E CSQJDS02 RECEIVED ERROR STATUS x FROM MMSVR CONNECT FOR DSNAME=xx • CSQJ144E Active log data set allocation error MQ will then skip over this encrypted log and move to the next un-encrypted log data set.
Shared Message Data Set (SMDS)	No	IEC161I-122 logged “The data set has a KEYLABEL, but the user did not specify that the application could handle encryption”. SMDS marked AVAIL(ERROR). Applying data set encryption to the SMDS can result in unexpected behaviour depending on the offload rules and potentially how full the structure is. For example if the SMDS status is not noticed at the time it is logged, an application error may not occur until an MQPUT of a message that requires offload is attempted. If the application only uses small messages, that offload may not occur until the CF structure is 80% full, which could be a significant time between the SMDS error being logged and MQPUTs failing as a result.
Archive Log **V800 onwards**	Yes	May require changes to ACS routines as these data sets are allocated dynamically. The Knowledge Center for IBM MQ 9.0.x has been updated to discuss encrypted archive logs.

Other data sets such as those used by DB2 for BLOB storage are not included in the table as SMDS is the preferred performance option for MQ.

Impact of encrypting MQ archive logs

In a previous blog “Reducing storage occupancy with IBM zEnterprise Data Compression“, the performance measurements compared a set of persistent workload with a range of message sizes from 2KB to 4MB when the archive logs were both compressed and uncompressed.

As a comparison, the tests were run in 3 configurations:

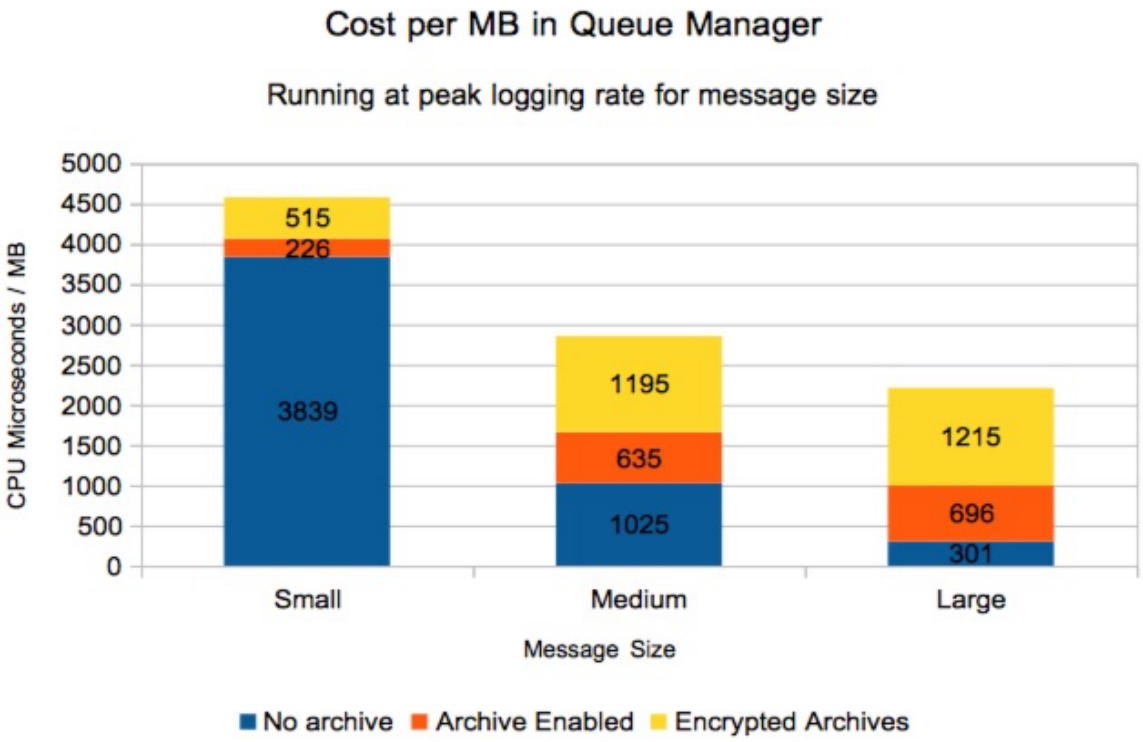
- No offload
- Offload to single archive log
- Offload to single archive log with encryption

The workload uses a simple set of batch request/reply tasks that drive the MQ logger task to its maximum capacity for specific message sizes.

Costs shown only include the queue manager since the application cost is not impacted by archiving or data set encryption.

The average write time of the archive data set increase by 35-50%, which may result in more archive processes running in parallel.

The following chart shows the impact of first enabling archiving and subsequently encrypted archives in the MQ queue manager address space.



Cost of Encrypting Archive Logs on IBM MQ for z/OS

As the peak logging rate increases with message size, the impact of both enabling archiving and encrypting the archives also increased due in part to contention when using the CPACF / CPU processors with the increased number of archive processes running in parallel.

For medium sized messages, the cost of offload to archives on z13 was 635 microseconds. Encrypting these archives added a further 1195 microseconds.

A rule of thumb would be that the cost of writing the encrypted archive is approximately 3 times the cost of just writing the archive on z13.

Workload rates were not affected as:

- there were sufficient active logs in the ring such that the queue manager was not impacted by the increased time to archive

- there is sufficient CPU such that the additional cost of encryption, which is performed by CPACF, does not impact the work running on the general purpose processors.